FUZZY-BASED MULTIPLE PATH SELECTION METHOD FOR IMPROVING ENERGY EFFICIENCY IN BANDWIDTH-EFFICIENT COOPERATIVE AUTHENTICATIONS OF WSNS

Su Man Nam[1] and Tae Ho Cho[2]

[1, 2]College of Information and Communication Engineering, Sungkyunkwan University, Suwon, 440-746, Republic of Korea

ABSTRACT

In wireless sensor networks, adversaries can easily compromise sensors because the sensor resources are limited. The compromised nodes can inject false data into the network injecting false data attacks. The injecting false data attack has the goal of consuming unnecessary energy in en-route nodes and causing false alarms in a sink. A bandwidth-efficient cooperative authentication scheme detects this attack based on the random graph characteristics of sensor node deployment and a cooperative bit-compressed authentication technique. Although this scheme maintains a high filtering probability and high reliability in the sensor network, it wastes energy in en-route nodes due to a multireport solution. In this paper, our proposed method effectively selects a number of multireports based on the fuzzy rule-based system. We evaluated the performance in terms of the security level and energy savings in the presence of the injecting false data attacks. The experimental results indicate that the proposed method improves the energy efficiency up to 10% while maintaining the same security level as compared to the existing scheme.

KEYWORDS

Wireless sensor network, Network security, bandwidth-efficient cooperative authentication scheme, fuzzy logic

1. INTRODUCTION

Wireless sensor networks (WSNs) have been applied in ubiquitous computing systems in order to monitor target environments [1]. A WSN consists of a large number of sensor nodes and a sink in a sensor field [2]. These sensor nodes detect environmental changes, generate data, and transmit the data to the sink. The sink collects the data transmitted from the sensor nodes and reports it to the users. Although the WSN is easily operated without infrastructure, the sensor nodes have the great disadvantage of possibly being captured and compromised due to their limited hardware resources (e.g., energy, memory, etc.). In addition, the sensor nodes are exposed to various attack patterns such as sinkhole [3], sybil [4], and wormhole [5] attacks. Thus, the sensor network is impractical for monitoring the environment when such attacks are generated.

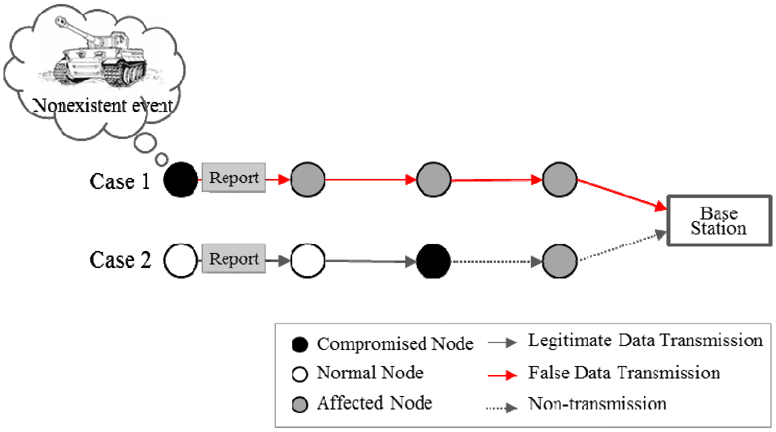

Figure1. Injecting false data attacks

WSNs are very vulnerable to various attacks because they are often deployed in unattended or hostile environments. One of the various attacks is the injecting false data attack [6]. As shown in Figure 1, an adversary compromises several sensor nodes, accesses all of the keys stored in these compromised nodes, and then controls the nodes to inject bogus information. If false reports with bogus information arrive at the sink, the en-route nodes consume unnecessary energy in communicating the false report. In addition, the compromised nodes can interrupt the forwarding of legitimate reports. Thus, the sensor network suffers a great loss as the injecting false data attack is generated in compromised nodes.

In order to detect an injecting false data attack, bandwidth-efficient cooperative authentication (BECAN) was proposed because of its high filtering probability and high reliability [6]. BECAN uses a cooperative neighbors × router-based (CNR) filtering mechanism for high filtering probability and a multireport solution (i.e., multiple paths) for high reliability. In BECAN, when a source node and its neighbors detect an event, the neighbors each generate a message authentication code (*mac*). The source node collects every mac and produces a *MAC* in a report. The report is forwarded through the multireport solution, which is transmitted along multiple routing paths. Although BECAN has high filtering probability and reliability compared to previous filtering mechanisms [7-9], the sensor node energy may be wasted in the en-route nodes due to the multireport solution.

In this paper, we propose a method to effectively select the number of multireports based on a fuzzy logic system. When a report is received at a sink, the sink determines the condition of the whole network considering three input factors using fuzzy logic. It then forwards the result of the fuzzy system to every node. The effective number of reports influences the high reliability and energy savings in the sensor network. The experimental results show that our proposed method improves the energy efficiency by effectively selecting the number of reports. Thus, our proposed method more effectively chooses the number of reports in order to improve the energy efficiency against the injecting false data attacks compared to the existing scheme.

The rest of this paper is organized as follows. The background and motivation of this study are described in Section 2. We introduce the details of our proposed method in Section 3. Section 4 provides the analysis and experimental results. The conclusions and future works are discussed at the end of this paper.

2. BACKGROUND AND MOTIVATION

2.1. Bandwidth-Efficient Cooperative Authentication Scheme (BECAN)

BECAN effectively detects false data that is injected in en-route node data based on the random graph characteristics of sensor deployment and a cooperative bit-compressed authentication technique. The random graph characteristics are used to select k neighbors for multireport solutions. The cooperative bit-compressed authentication technique is used for detecting false data in the en-route nodes. BECAN consists of four phases: (1) sensor nodes initialization and deployment, (2) sensed results reporting protocol, (3) en-routing filtering, and (4) sink verification.

In phase (1), the sensor node initialization and deployment, the sink selects an elliptic curve $\mathrm{E}\left(\left(IF_p\right), G, q\right)$ and a hash function h(). It then sets the public parameters (*params*) as follows:

$$\text{params} = \{\mathrm{E}(IF_p, G, q, h()\}$$

Every sensor node sets TinyECC[10] and *params* before they are deployed in the sensor field as follows:

$$\begin{aligned} \text{params} = \{&\mathrm{E}(IF_p, G, q, h()\} \\ &p{:}\, a\ large\ prime, h{:}\, \{0, 1\} \\ &G \in E\left(IF_p\right){:}\, a\ base\ point\ of\ prime\ order\ q\ with\ |q| = k \end{aligned}$$

Each node is randomly assigned a private key () (where the private key x_i is randomly chosen from z_p^*), while all nodes collectively generate the public key Y_i ($Y_i = x_i G$, where i is a node's identifier.) Thus, each node has a public key and a private key (Y_i, x_i).

In phase (2), the sensed results reporting phase, it is assumed that a source node N_0 establishes a routing path $R_{N_0}{:}\{R_1 \rightarrow R_2 \rightarrow \cdots \rightarrow R_l \rightarrow Sink\}$. When a real event occurs, the source node obtains a current timestamp *T* for generating a message *m*. The source collects the *mac* (*m, T*) from the neighbors and verifies the message *m* and the timestamp *T*. The source node then generates a report including the data (*m, T, MAC*) and selects *k* different neighbors to use the multireport solution to forward the report along multiple routing paths.

In phase (3), en-route filtering, when the en-route nodes receive the report, they determine the integrity of the message *m* and the timestamp *T*. The report (*m, T, MAC*) is then discarded. If the timestamp is normal, the en-route nodes verify the *MAC* in the report using the public key and the CNR-based *MAC* verification algorithm. If the report is legitimate, the report is transmitted to the next hop node.

In phase (4), sink verification, when a sink receives the report, it verifies the message and timestamp, as well as the *MAC*. If one report reaches the sink, the legitimate event is successfully reported.

2.2. Motivation

In an open WSN environment, compromised nodes can generate an injecting false data attack to generate false reports with bogus information. BECAN achieves both high filtering probability and high reliability against those attacks. This scheme uses a cooperative bit-compressed authentication technique with a high filtering probability to filter out the injected false data. To improve the reliability, this scheme uses multireports, where multiple reports are generated in the source nodes to be forwarded along their paths to the sink. Although the existing method provides high filtering probability and high reliability in the sensor network, the sensors may waste energy in the en-route nodes due to the multiple reports. In this paper, our proposed method effectively selects a number of multireports using three factors regarding the network condition based on a fuzzy logic system. Thus, the proposed method selects the effective number of reports in order to enhance the energy efficiency against attacks as compared to BECAN.

3. PROPOSED METHOD

3.1. Assumption

In this paper, a sensor network consists of a sink and sensor nodes (e.g., H-sensors and L-sensors [11, 12]). The H-sensors' hardware resources (CPU, memory, storage, etc.) are more powerful than those of L-sensors. After deploying the sensor nodes in the sensor field, the sensor network enables H-sensors to serve as cluster heads (CHs) and to clusters around the CHs with L-sensors. The topology then establishes the initial routing paths using directed diffusion [13] and a minimum cost forwarding algorithm [14]. The CHs discover a routing path toward the sink. We further assume that a compromised node injects false reports and interrupts legitimate reports in the sensor network.

3.2. Overview

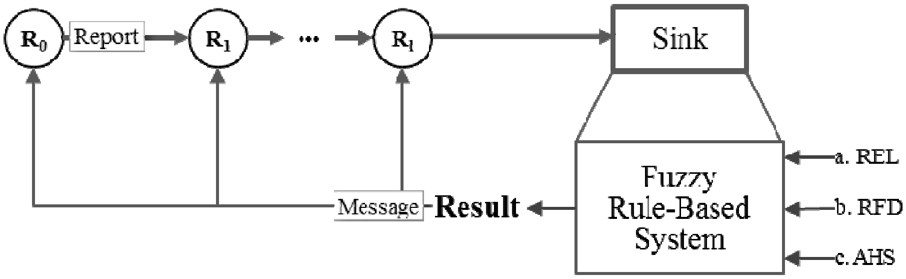

Figure2. Overview of the proposed fuzzy rule-based system

Our proposed method detects injecting false data attacks and effectively selects the number of multireports based on a fuzzy rule-based system. Figure 2 shows the proposal's processes for executing the fuzzy rule-based system with three input factors. When an event occurs in a sensor field, a source node produces a report to be forwarded to the sink. After the sink receives the report, the fuzzy system is used to determine the condition of the sensor network. The result that is obtained from the fuzzy system is forwarded to every node. Using the result message, neighboring nodes apply the number of multireports as a report is transmitted. Thus, our proposed method effectively determines the number of multireports according to the condition of the network based on the fuzzy rule-based system.

3.3. Proposed Method using Fuzzy Logic

The input factors of the fuzzy logic system are as follows:

- Remaining energy level (REL): This value is an important factor in reducing needless energy consumption in the sensor network. If the energy level of the whole network is very low, the number of transmitted multireports should be reduced in order to decrease unnecessary energy consumption in the sensor network. The improvement in energy efficiency is influenced by the number of the reports transmitted.
- Ratio of false data filtered by en-route nodes (RFD): This factor represents the security of the whole network. If the ratio is high, the network maintains high reliability because the compromised nodes are injecting much false data. The security level is influenced by the ratio of filtered false data.
- Average number of hops of source nodes (AHP): This factor describes the hop count, which is the number of nodes traveled en-route from the source node. With a long distance from the source to the sink, reports transmitted via multiple hops consume a great deal of the energy of the en-route nodes. The network's energy resource is influenced by high numbers of hops in the en-route nodes.

The output factor is as follows:

- Result (RST): This value determines the number of report transmissions of the source nodes. If the value is five, the report should be forwarded to five neighboring nodes of the source node. The effective selection of the value is influenced by three input factors based on the fuzzy rule-based system.

Figures 3, 4, 5, and 6 show the membership function of the fuzzy logic input and output parameters. The labels of the input fuzzy variables are as follows:

- REL = {VS (very small), SM (small), MD (medium), MN (many), VM (very many)}
- RFD = {LW (low), MD (moderate), HG (high)}
- AHP = {NR (near), MD (moderate), FR (far)}

The logic output parameter is represented by a label. The label values are as follows:

- RST = {TW (two), TH (three), FR (four), FV (five)}
-

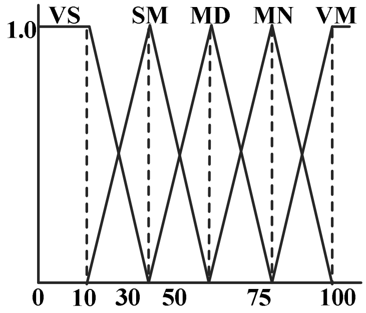

Figure3. REL of the fuzzy membership function

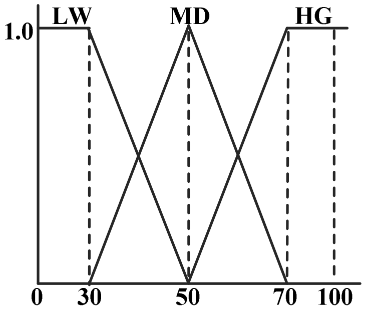

Figure 4. RFD of the fuzzy membership function

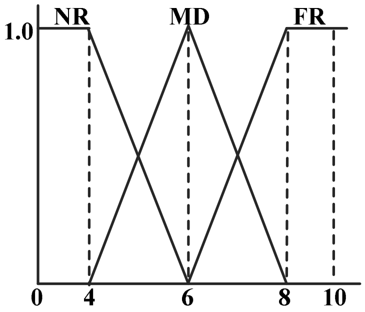

Figure5. AHP of the fuzzy membership function

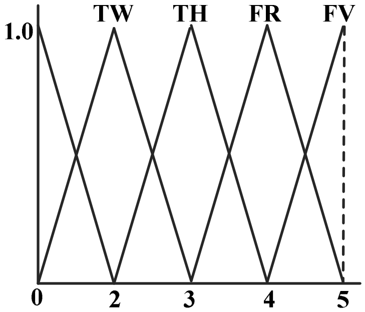

Figure 6. RST of the fuzzy membership function

Table 1 shows the 45 (= 5 × 3 × 3) rules of the fuzzy system. If REL is very small, RFD, is low, and AHS is near, then the number of multireports is two (TW), such as for *Rule 0*. This case indicates that there is a normal state to forward the multireports in a source node. In contrast, if REL is very large, RFD is large, and AHS is far, then the number of multireports is five (FV), such as for *Rule 44*. This case indicates that there is an abnormal condition due to injecting false data attacks. The sensor network needs to effectively select the number of multireports in order to improve the energy efficiency.

Table 1. Fuzzy if-then rules

Rule no.	**IF**			**THEN**
	REL	**RFD**	**AHS**	**RST**
0	VS	SM	NR	TW
1	VS	SM	MD	TW
2	VS	SM	FR	TW
3	VS	MD	NR	TW
4	VS	MD	MD	TW
5	VS	MD	FR	TH
6	VS	LG	NR	TH
7	VS	LG	MD	TH
8	VS	LG	FR	TH
⋮				
43	VL	LG	MD	FV
44	VL	LG	FR	FV

4. EXPERIMENTAL RESULTS

Experiments were performed to determine the effectiveness of the proposed method compared to BECAN. The sensor network environment is 500×500 m^2 and includes a total of 500 nodes (100 CHs and 400 normal nodes) in the sensor field. The nodes are uniformly distributed. A cluster consists of one cluster node and four normal nodes. In [7], the sensors consume 16.25 µJ to transmit each byte and 12.5 µJ to receive each byte. They also consume 15 µJ and 75 µJ, respectively, to generate and verify a *MAC*. We randomly generated 1,000 events. The message and report sizes are 1 byte and 24 bytes, respectively. For injecting false data attacks, five sensor nodes are compromised after deployment in the field. The compromised node injects false reports by using 5% probability into the network.

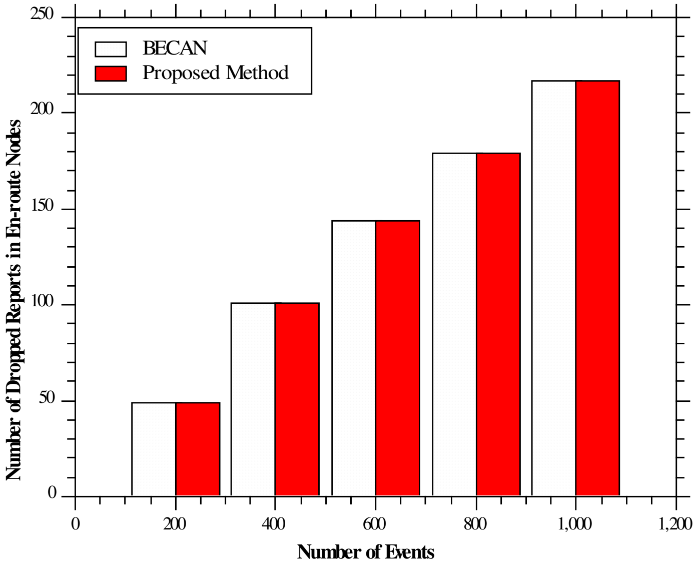

Figure.7 Number of dropped reports in adversary nodes versus number of events

Figure 7 shows the number of dropped false reports in the en-route nodes in terms of the number of events. As shown in Figure 7, BECAN and the proposed method have the same number of dropped reports. The compromised nodes drop 217 false reports for both methods when 1,000 events are generated. Therefore, the proposed method maintains the same security level as BECAN.

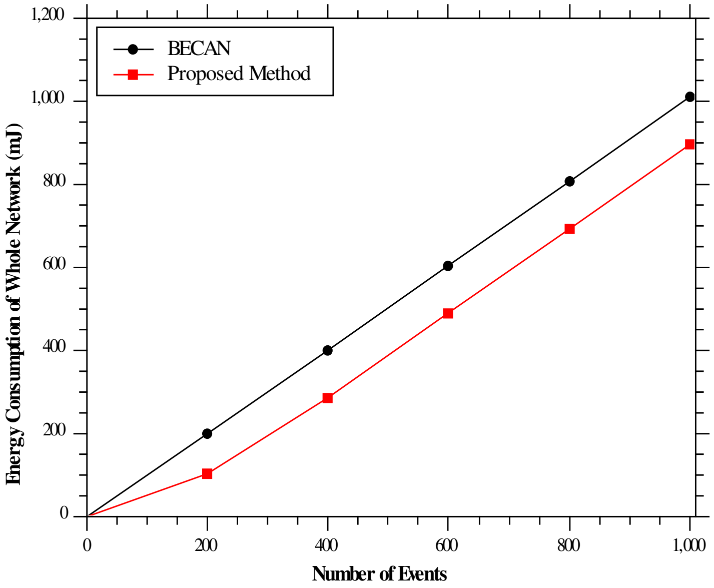

Figure 8. Energy consumption of the whole network versus number of events

Figure 8 shows the energy consumption of the whole network in terms of the number of events. When 200 events occur, a difference in energy consumption exists between BECAN and the proposed method. When 1,000 events are generated, BECAN and the proposed method consume 1,010 mJ and 987 mJ, respectively. The reason for this difference is that the effective number of multireports is selected through the network's condition based on the fuzzy rule-based system. The proposed method improves the energy savings up to about 10% compared to BECAN. Therefore, our proposed method saves energy resources through the effective selection of the number of multireports and prolongs the sensor network lifetime.

5. CONCLUSIONS AND FUTURE WORKS

In WSNs, sensor nodes are easily compromised by an adversary because their hardware has limited constraints. The compromised nodes consume unnecessary energy in the sensor network when injecting false data attacks are generated. In addition, other en-route compromised nodes can inject bogus information into a legitimate report. BECAN detects this attack based on the random graph characteristics of sensor node deployment and using a cooperative bit-compressed authentication technique. This existing scheme maintains both high filtering probability and high reliability against such attacks. However, BECAN wastes unnecessary energy in en-route nodes due to the multireport solution. Our proposed method effectively chooses the number of multireports based on a fuzzy rule-based system. We use three input factors to measure the network condition and to determine the effective number of multireports. The experimental results demonstrate that the proposed method saves up to 10% of the energy resources while maintaining the same security level compared to the existing scheme. Therefore, our proposed method conserves the energy resources of the whole network and prolongs the network's lifetime. In the future, we propose optimization of the fuzzy rule-based system in the proposed method in order to operate an optimal sensor network.

ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2013R1A2A2A01013971).

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam & E. Cayirci, (2002) "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, pp. 102-114.

[2] K. Akkaya and M. Younis, (2005) "A survey on routing protocols for wireless sensor networks," Ad Hoc Networks, vol. 3, pp. 325-349.

[3] E. C. H. Ngai, J. Liu and M. R. Lyu, (2007) "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," vol. 30, pp. 2353-2364.

[4] Jing Deng, Richard Han and Shivakant Mishra, (2006) "INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks," Computer Communications, vol. 29, pp. 216-230.

[5] Ji-Hoon Yun, Il-Hwan Kim, Jae-Han Lim and Seung-Woo Seo, (2006) "WODEM: wormhole attack defense mechanism in wireless sensor networks," ICUCT'06 Proceedings of the 1st International Conference on Ubiquitous Convergence Technology, pp. 200-209.

[6] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang and Xuemin Shen, (2012) "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," Parallel and Distributed Systems, IEEE Transactions On, vol. 23, pp. 32-43.

[7] F. Ye, H. Luo, S. Lu and L. Zhang, (2005) "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal On, vol. 23, pp. 839-850.

[8] S. Zhu, S. Setia, S. Jajodia and P. Ning, (2004) "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium On, pp. 259-271.
[9] H. Yang, F. Ye, Y. Yuan, S. Lu and W. Arbaugh, (2005) "Toward resilient security in wireless sensor networks," in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Urbana-Champaign, IL, USA, pp. 34-45.
[10] Xiaojiang Du, M. Guizani, Yang Xiao and Hsiao-Hwa Chen, (2007) "Two Tier Secure Routing Protocol for Heterogeneous Sensor Networks," Wireless Communications, IEEE Transactions On, vol. 6, pp. 3395-3401.
[11] MICAz., http://bullseye.xbow.com:81/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf.
[12] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed Diffusion: A scalable and robust communication paradigm for sensor networks," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pp. 56-67, 2000.
[13] F. Ye, A. Chen, S. Lu and L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks," in Computer Communications and Networks, 2001. Proceedings. Tenth International Conference On, 2001, pp. 304-309.

Authors

Su Man Nam received his B.S. degree in Computer Information from Hanseo University, Korea, in February 2009 and his M.S. degree in Electrical and Computer Engineering from Sungkyunkwan University in 2013. He is currently a doctoral student in the College of Information and Communication Engineering at Sungkyunkwan University, Korea. His research interests include wireless sensor networks, security in wireless sensor networks, and modeling & simulation.

Tae Ho Cho received a Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Republic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Information and Communication Engineering, Sungkyunkwan University, Korea. His research interests are in the areas of wireless sensor networks, intelligent systems, modeling & simulation, and enterprise resource planning.